



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

*Am*

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

7590 06/14/2005

W. Scott Petty, Esq.  
KING & SPALDING  
45th Floor  
191 Peachtree Street, N.E.  
Atlanta, GA 30303

EXAMINER

SON, LINH L D

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/844,448

Applicant(s)

HOUSTON ET AL.

Examiner

Linh LD Son

Art Unit

2135

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 April 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-59 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-59 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This Office Action is responding to the amendment dated 02/22/05
2. Claims 1, 16, 27-28, 34, 49 are amended.
3. Claims 1-59 are pending.
4. Applicant requests an approval for the telephonic interview summary, dated 02/17/05, in the remark. Examiner verified that the interview summary written in the remark is consistence with the record. Examiner considers the interview summary in the remark.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-11, 13-22, 24-44, 46-55, and 57-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al, US Patent No. 6088804, hereinafter "Hill", *cited in IDS 6/24/03*
7. As per claims 1, 18 and 49, Hill discloses "A method for managing security event data collected from a security devices in a distributed computing environment" in (Figure

Art Unit: 2135

1) "comprising the steps of: generating a plurality of alerts with a plurality of security devices at a first location" in (Col 4 lines 30-40); "creating scope criteria by adjusting variables operable for analyzing security event data, the security event data comprising the plurality of alerts" in (Col 5 lines 25-45); "collecting security event data generated by the plurality of security devices located at a first location" in (Col 4 lines 30-40); "storing the collected security event data at a second location" in (Col 8 lines 12-19); and "analyzing the collected security event data with the scope criteria to produce result data, the result data accessible by a plurality of clients" in (Col 5 lines 15-20, and lines 20-45, Col 8 lines 4-11, and Col 8 line 63 to Col 9 line 7).

8. As per claims 2, 21, 35, and 54, Hill discloses the method of claims 1, 16, 34, and 49, further comprising storing one or more of the scope criteria, the security event data, and the result data in a database (Col 8 lines 12-19).

9. As per claim 3, 5, 18-20, 30 and 36, Hill discloses "the method of claims 1, 16, and 27, wherein the first location is a distributed computing environment (Figure 1), the second location is a database server (Col 8 lines 12-19), and the third location is an application server (Col 5 lines 15-20) to which the plurality of clients are coupled".

10. As per claims 4, 14, 19, 38, 47, and 53, Hill discloses "the method of claims 1, 16, 34, and 49, wherein collecting the security event data comprises generating security event data from a sensor" in (Col 4 lines 30-40); "sending the security event data from

Art Unit: 2135

the sensor to a collector” in (Col 8 lines 12-19); and “converting the event data to a common format” in (Col 5 lines 37).

11. As per claims 6 and 39, Hill discloses “the method of claims 1 and 35, further comprising searching the stored security event data for additional information identifying a security event” in (Col 5 lines 26-45).

12. As per claims 7 and 40, Hill discloses “the method of claims 1 and 35, further comprising: polling a database server for current stored security event data; analyzing the current stored security event data to produce current result data; and rendering the current result data” in (Col 5 lines 26-45).

13. As per claims 8 and 41, Hill discloses the method of claims 1 and 34, further comprising polling for messages containing information about scope criteria, security event data, or result data (Col 5 lines 26-45).

14. As per claims 9 and 42, Hill discloses the method of claims 1 and 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data (Col 4 lines 30-40, and Col 8 lines 4-11).

Art Unit: 2135

15. As per claims 10, 17, 43, and 50, Hill discloses the method of claims 1, 16, 34, and 49, wherein the step of rendering result data comprises presenting the result data in a chart format (Figure 7).

16. As per claims 11, 22, 44, and 55, Hill discloses the method of claims 1, 16, and 34, wherein in response to analyzing the collected security event data, an action is executed (Col 7 line 63 to Col 8 line 12).

17. As per claims 13, 24, 46, and 57, Hill discloses the method of claims 11, 22, 44, and 55, wherein the action is creating an incident from result data for preparing a response (Col 7 line 63 to Col 8 line 12).

18. As per claims 15, 26-27, 48, and 59, Hill discloses "A computer-implemented system for managing security event data collected from a plurality of security devices comprising: a plurality of security devices operable for generating security event data comprising a plurality of alerts" in (Col 4 lines 3-40); "an event manager coupled to the security devices, the even manager operable for collecting security event data from the security devices and analyzing the security event data with scope criteria comprising a plurality of defineable variables operable for analyzing the security event data" in (Fig 1, Col 8 lines 14-19, and Col 5 lines 7-45); and "a client coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager" in (Col 7 line 64 to Col 8 line 11).

19. As per claims 16, and 34, the rejection basis of claims 1, and 27 is incorporate. Further, Hill discloses applying the scope criteria to the security event data at a third location to produce a result, the result accessible by a plurality of clients coupled to a server” in (Fig 1, Col 8 lines 15-35, and Col 5 lines 45-65).

20. As per claims 25, and 51, Hill discloses “the method of claim 16, and 49, further comprising applying additional scope criteria to a plurality of results” in (Col 7 lines 40-63).

21. As per claim 28, Hill discloses “the system of claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data” in (Col 8 lines 12-19, and Col 7 lines 45-65)

22. As per claim 29, Hill discloses the system of claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response (Col 8 lines 1-21).

23. As per claim 31, Hill discloses the system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager (Col 8 lines 1-21).

Art Unit: 2135

24. As per claim 32, Hill discloses the method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data (Figure 7).

25. As per claim 33, Hill discloses the method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients (Figure 7).

26. As per claim 37, Hill discloses the method of Claim 34, further comprising editing the scope criteria (Col 5 lines 1-6 and Col 5 lines 25-38).

27. As per claims 37, and 51, Hill discloses the method of Claims 1, and 49, further comprising the step of creating and editing the scope criteria for filtering the security event data (Col 5 lines 1-6, and Col 5 lines 25-38).

### ***Claim Rejections - 35 USC § 103***

28. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

29. Claims 12, 23, 45, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hill.



30. As per claims 12, 23, 45, and 56, Hill discloses the method of claims 11, 22, and 44. However, Hill does not mention the action is clearing security event data from storage. Nevertheless, it would have been obvious at the time of the invention for one having ordinary skill in the art to realize that the capability of clearing out the data must be exist in the invention of Hill, since it is inevitable to contain unlimited data in any storage devices.

#### ***Response to Amendment***

31. Applicant has amended claims 1, 16, 27-28, 34, 49, which necessitated new grounds of rejection. See Rejections above.

#### ***Conclusion***

32. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2135

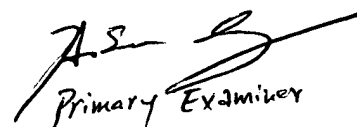
the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

**Conclusion**

33. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-272-3856.

34. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

35. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see <http://pzr-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Primary Examiner  
AU 2135